

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-303945  
 (43)Date of publication of application : 13.11.1998

(51)Int.Cl. H04L 12/40  
 G11B 20/10  
 H04L 9/08  
 H04L 9/14  
 H04L 9/16  
 H04L 12/56

(21)Application number : 09-106105  
 (22)Date of filing : 23.04.1997

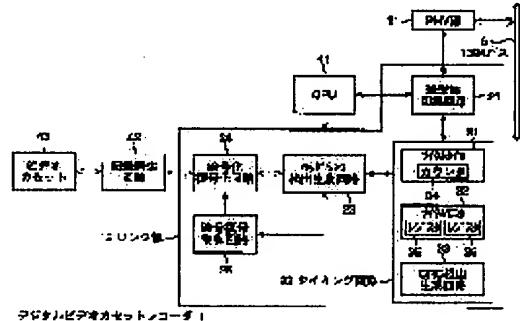
(71)Applicant : SONY CORP  
 (72)Inventor : OSAKABE YOSHIO  
 SATO MAKOTO  
 OSAWA YOSHITOMO  
 ASANO TOMOYUKI  
 ISHIGURO RYUJI  
 SHIMA HISATO

**(54) DATA TRANSMITTING DEVICE AND METHOD, DATA RECEIVING DEVICE AND METHOD, DATA TRANSMITTING/RECEIVING SYSTEM AND METHOD**

**(57)Abstract:**

**PROBLEM TO BE SOLVED:** To prevent unauthorized utilization of data.

**SOLUTION:** The data to be transmitted with a 1394 bus 5 is ciphered by a ciphering and deciphering circuit 24 and a header is added to the data by a header sync detecting and generating circuit 23. After a CRC is added to the data by a CRC detecting and generating circuit 33, the data is packetted to an isochronous packet in an isochronous mode by a transmission/reception switching circuit 21. Among ciphering keys, a session key is transmitted by a packet in an asynchronous mode and a time variable key is transmitted by a packet in the isochronous mode.



**LEGAL STATUS**

[Date of request for examination] 06.11.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3760460  
[Date of registration] 20.01.2006  
[Number of appeal against examiner's decision of rejection]  
[Date of requesting appeal against examiner's decision of rejection]  
[Date of extinction of right]

特開平10-303945

(43)公開日 平成10年(1998)11月13日

(51) Int.Cl. <sup>6</sup>	識別記号	F I
H 04 L 12/40	H 04 L 11/00	3 2 0
G 11 B 20/10	G 11 B 20/10	H
		D
H 04 L 9/08	H 04 L 9/00	6 0 1 C
9/14		6 4 1

審査請求 未請求 請求項の数21 OL (全 11 頁) 最終頁に続く

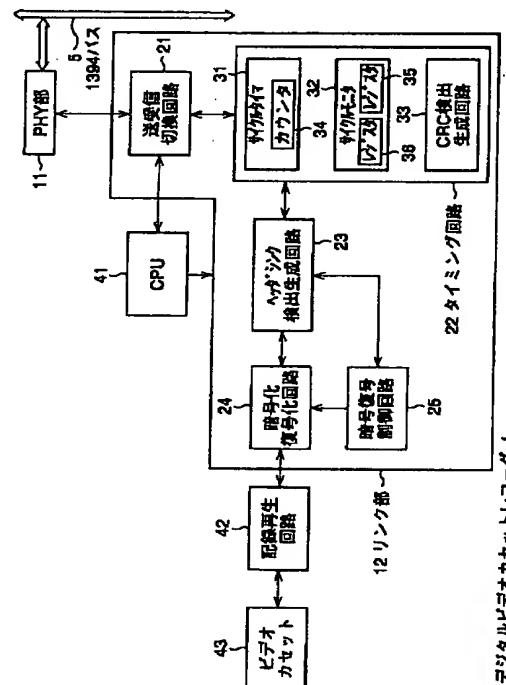
(21)出願番号	特願平9-106105	(71)出願人	000002185 ソニーブル株式会社 東京都品川区北品川6丁目7番35号
(22)出願日	平成9年(1997)4月23日	(72)発明者	刑部 義雄 東京都品川区北品川6丁目7番35号 ソニーブル株式会社内
		(72)発明者	佐藤 真 東京都品川区北品川6丁目7番35号 ソニーブル株式会社内
		(72)発明者	大澤 義知 東京都品川区北品川6丁目7番35号 ソニーブル株式会社内
		(74)代理人	弁理士 稲本 義雄
			最終頁に続く

(54)【発明の名称】 データ送信装置および方法、データ受信装置および方法、並びにデータ送受信システムおよび方法

## (57)【要約】

【課題】 データの不正な利用を防止する。

【解決手段】 1394バス5を介して伝送するデータを、暗号化復号化回路24で暗号化し、ヘッダシンク検出生成回路23でヘッダを付加する。CRC検出生成回路33でCRCを付加した後、送受信切換回路21でアイソクロナスマードのアイソクロナスパケットにパケット化する。暗号鍵のうち、セッションキーは、アシンクロナスマードのパケットで伝送し、時変キーは、アイソクロナスマードのパケットで伝送する。



## 【特許請求の範囲】

【請求項1】 アイソクロナスマードとアシンクロナスマードとを有するシリアルバスで接続された情報処理装置にデータを送信するデータ送信装置において、送信するデータを暗号鍵を用いて暗号化する暗号化手段と、前記暗号化手段により暗号化されたデータを、前記アイソクロナスマードのパケットにパケット化するパケット化手段と、前記パケット化手段によりパケット化されたデータを前記シリアルバスに送信する送信手段とを備えることを特徴とするデータ送信装置。

【請求項2】 前記パケットのヘッダに、前記暗号化に関する識別コードを記録する記録手段をさらに備えることを特徴とする請求項1に記載のデータ送信装置。

【請求項3】 前記暗号鍵は、送信するデータの各セッションにおいて不变なセッションキーと、前記セッション内において更新される時変キーとからなることを特徴とする請求項1に記載のデータ送信装置。

【請求項4】 前記時変キーに関する情報を、前記アイソクロナスマードのパケットに記録する記録手段をさらに備えることを特徴とする請求項3に記載のデータ送信装置。

【請求項5】 前記記録手段は、前記時変キーに関する情報を、前記パケットのヘッダに記録することを特徴とする請求項4に記載のデータ送信装置。

【請求項6】 前記パケットに含ませるデータから所定のデータを前記時変キーとして抽出する抽出手段をさらに備えることを特徴とする請求項3に記載のデータ送信装置。

【請求項7】 前記時変キーとして抽出するデータを含ませる前記パケットは、前記シリアルバスにおいて、各アイソクロナスマイルのスタートのタイミングを表すスタートパケットであることを特徴とする請求項6に記載のデータ送信装置。

【請求項8】 前記セッションキーに関する情報を、前記アシンクロナスマードのパケットに記録する記録手段をさらに備えることを特徴とする請求項3に記載のデータ送信装置。

【請求項9】 前記暗号鍵に関する情報を、前記シリアルバスにおいて、各アイソクロナスマイルのスタートのタイミングを表すスタートパケットに記録する記録手段をさらに備えることを特徴とする請求項1に記載のデータ送信装置。

【請求項10】 アイソクロナスマードとアシンクロナスマードとを有するシリアルバスで接続された情報処理装置にデータを送信するデータ送信方法において、送信するデータを暗号鍵を用いて暗号化する暗号化ステップと、前記暗号化ステップにより暗号化されたデータを、前記

アイソクロナスマードのパケットにパケット化するパケット化ステップと、前記パケット化ステップでパケット化されたデータを前記シリアルバスに送信する送信ステップとを備えることを特徴とするデータ送信方法。

【請求項11】 アイソクロナスマードとアシンクロナスマードとを有するシリアルバスで接続されたデータ送信装置から送信されてきたデータを受信するデータ受信装置において、

前記シリアルバスを介して送信されてきたデータを受信する受信手段と、前記アイソクロナスマードのパケットにパケット化されているデータをデパケット化するデパケット化手段と、前記アイソクロナスマードのパケットをデパケット化して得たデータであって、暗号化されているデータを復号する復号手段とを備えることを特徴とするデータ受信装置。

【請求項12】 前記パケットのヘッダから、前記暗号化に関する識別コードを抽出する抽出手段をさらに備えることを特徴とする請求項11に記載のデータ受信装置。

【請求項13】 前記暗号鍵は、送信するデータの各セッションにおいて不变なセッションキーと、前記セッション内において更新される時変キーとからなることを特徴とする請求項11に記載のデータ受信装置。

【請求項14】 前記時変キーに関する情報を、前記アイソクロナスマードのパケットから抽出する抽出手段をさらに備えることを特徴とする請求項13に記載のデータ受信装置。

【請求項15】 前記抽出手段は、前記時変キーに関する情報を、前記パケットのヘッダから抽出することを特徴とする請求項14に記載のデータ受信装置。

【請求項16】 前記抽出手段は、前記パケットのデータから所定のデータを前記時変キーとして抽出することを特徴とする請求項14に記載のデータ受信装置。

【請求項17】 前記抽出手段が前記時変キーを抽出する前記パケットは、前記シリアルバスにおいて、各アイソクロナスマイルのスタートのタイミングを表すスタートパケットであることを特徴とする請求項16に記載のデータ受信装置。

【請求項18】 前記セッションキーに関する情報を、前記アシンクロナスマードのパケットから抽出する抽出手段をさらに備えることを特徴とする請求項13に記載のデータ受信装置。

【請求項19】 アイソクロナスマードとアシンクロナスマードとを有するシリアルバスで接続されたデータ送信装置から送信されてきたデータを受信するデータ受信方法において、

前記シリアルバスを介して送信されてきたデータを受信する受信ステップと、

前記アイソクロナスマードのパケットにパケット化されているデータをデパケット化するデパケット化ステップと、

前記アイソクロナスマードのパケットをデパケット化して得たデータであって、暗号化されているデータを復号する復号ステップとを備えることを特徴とするデータ受信方法。

【請求項20】アイソクロナスマードとアシンクロナスマードとを有するシリアルバスで接続されたデータ送信装置と、前記データ送信装置が送信したデータを受信するデータ受信装置とを備えるデータ送受信システムにおいて、

前記データ送信装置は、

送信するデータを暗号鍵を用いて暗号化する暗号化手段と、

前記暗号化手段により暗号化されたデータを、前記アイソクロナスマードのパケットにパケット化するパケット化手段と、

前記パケット化手段によりパケット化されたデータを前記シリアルバスに送信する送信手段とを備え、

前記データ受信装置は、

前記シリアルバスを介して送信されてきたデータを受信する受信手段と、

前記アイソクロナスマードのパケットにパケット化されているデータをデパケット化するデパケット化手段と、前記アイソクロナスマードのパケットをデパケット化して得たデータであって、暗号化されているデータを復号する復号手段とを備えることを特徴とするデータ送受信方法。

【請求項21】アイソクロナスマードとアシンクロナスマードとを有するシリアルバスで接続されたデータ送信装置と、前記データ送信装置から送信したデータを受信するデータ受信装置とを備えるデータ送受信システムのデータ送受信方法において、

前記データ送信装置は、

送信するデータを暗号鍵を用いて暗号化する暗号化ステップと、

前記暗号化ステップにより暗号化されたデータを、前記アイソクロナスマードのパケットにパケット化するパケット化ステップと、

前記パケット化ステップによりパケット化されたデータを前記シリアルバスに送信する送信ステップとを備え、前記データ受信装置は、

前記シリアルバスを介して送信されてきたデータを受信する受信ステップと、

前記アイソクロナスマードのパケットにパケット化されているデータをデパケット化するデパケット化ステップと、

前記アイソクロナスマードのパケットをデパケット化して得たデータであって、暗号化されているデータを復号

する復号ステップとを備えることを特徴とするデータ受信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、データ送信装置および方法、データ受信装置および方法、並びにデータ送受信システムおよび方法に関し、特に、1394シリアルバスを利用してデータを送受信する場合において、データが不正に利用されるのを防止するようにした、データ送信装置および方法、データ受信装置および方法、並びにデータ送受信システムおよび方法に関する。

【0002】

【従来の技術】最近、IEEEで規定しているIEEE1394ハイパフォーマンスシリアルバス（以下、単に1394バスと称する）が普及しつつある。この1394バスにおいては、そこに、いわゆるAV機器や、パーソナルコンピュータなどの電子機器を接続することにより、高速にデジタルの映像や音声信号を制御コマンドとともに、実時間で1本のケーブルで伝送することができる。

【0003】

【発明が解決しようとする課題】1394バスにおいて、データを伝送するのに、アシンクロナスマード（非同期データ伝送モード）と、1394バスのサイクルマスターが発生する8kHz（125μs）のアイソクロナスマスクル同期するアイソクロナスマード（同期データ伝送モード）がある。コマンドは、アシンクロナスマードで伝送されることが多いが、映像信号や音声信号は、実時間で再生する必要があるため、通常、アイソクロナスマードで伝送される。

【0004】しかしながら、このアイソクロナスマードにおける伝送は、データの送信先を指定しない、いわゆる同報通信で行われる。このため、著作権の保護を受けるべき映像信号や音声信号が1394バスに伝送されてしまうと、著作権者からの許諾を得ていないユーザが、不正に映像信号や音声信号をコピーしたり、これをを利用して、変更や修正を加える恐れがある。

【0005】本発明はこのような状況に鑑みてなされたものであり、不正な利用を、より確実に防止することができるようとするものである。

【0006】

【課題を解決するための手段】請求項1に記載のデータ送信装置は、送信するデータを暗号鍵を用いて暗号化する暗号化手段と、暗号化手段により暗号化されたデータを、アイソクロナスマードのパケットにパケット化するパケット化手段と、パケット化手段によりパケット化されたデータをシリアルバスに送信する送信手段とを備えることを特徴とする。

【0007】請求項10に記載のデータ送信方法は、送信するデータを暗号鍵を用いて暗号化する暗号化ステップと、暗号化ステップにより暗号化されたデータを、ア

イソクロナスモードのパケットにパケット化するパケット化ステップと、パケット化ステップでパケット化されたデータをシリアルバスに送信する送信ステップとを備えることを特徴とする。

【0008】請求項11に記載のデータ受信装置は、シリアルバスを介して送信されてきたデータを受信する受信手段と、イソクロナスモードのパケットにパケット化されているデータをデパケット化するデパケット化手段と、イソクロナスモードのパケットをデパケット化して得たデータであって、暗号化されているデータを復号する復号手段とを備えることを特徴とする。

【0009】請求項19に記載のデータ受信方法は、シリアルバスを介して送信されてきたデータを受信する受信ステップと、イソクロナスモードのパケットにパケット化されているデータをデパケット化するデパケット化ステップと、イソクロナスモードのパケットをデパケット化して得たデータであって、暗号化されているデータを復号する復号ステップとを備えることを特徴とする。

【0010】請求項20に記載のデータ送受信システムは、データ送信装置は、送信するデータを暗号鍵を用いて暗号化する暗号化手段と、暗号化手段により暗号化されたデータを、イソクロナスモードのパケットにパケット化するパケット化手段と、パケット化手段によりパケット化されたデータをシリアルバスに送信する送信手段とを備え、データ受信装置は、シリアルバスを介して送信されてきたデータを受信する受信手段と、イソクロナスモードのパケットにパケット化されているデータをデパケット化するデパケット化手段と、イソクロナスモードのパケットをデパケット化して得たデータであって、暗号化されているデータを復号する復号手段とを備えることを特徴とする。

【0011】請求項21に記載のデータ送受信方法は、データ送信装置は、送信するデータを暗号鍵を用いて暗号化する暗号化ステップと、暗号化ステップにより暗号化されたデータを、イソクロナスモードのパケットにパケット化するパケット化ステップと、パケット化ステップによりパケット化されたデータをシリアルバスに送信する送信ステップとを備え、データ受信装置は、シリアルバスを介して送信されてきたデータを受信する受信ステップと、イソクロナスモードのパケットにパケット化されているデータをデパケット化するデパケット化手段と、イソクロナスモードのパケットをデパケット化して得たデータであって、暗号化されているデータを復号する復号ステップとを備えることを特徴とする。

【0012】請求項1に記載のデータ送信装置および請求項10に記載のデータ送信方法においては、暗号化されたデータが、イソクロナスモードのパケットにパケット化されて送信される。

【0013】請求項11に記載のデータ受信装置および請求項19に記載のデータ受信方法においては、イソクロナスモードのパケットでパケット化して得たデータであって、暗号化されているデータが復号される。

【0014】請求項20に記載のデータ送受信システムおよび請求項21に記載のデータ送受信方法においては、データ送信装置が、暗号化したデータを、イソクロナスモードのパケットにパケット化して、シリアルバスでデータ受信装置に送信する。データ受信装置は、アイソクロナスモードのパケットでパケット化して得たデータであって、暗号化されているデータを復号する。

#### 【0015】

【発明の実施の形態】以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【0016】請求項1に記載のデータ送信装置は、送信するデータを暗号鍵を用いて暗号化する暗号化手段（例えば、図2の暗号化復号化回路24）と、暗号化手段により暗号化されたデータを、イソクロナスモードのパケットにパケット化するパケット化手段（例えば、図2の送受信切換回路21）と、パケット化手段によりパケット化されたデータをシリアルバスに送信する送信手段（例えば、図2のPHY部11）とを備えることを特徴とする。

【0017】請求項2に記載のデータ送信装置は、パケットのヘッダに、暗号化に関する識別コードを記録する記録手段（例えば、図2の暗号復号制御回路25）をさらに備えることを特徴とする。

【0018】請求項4に記載のデータ送信装置は、時変キーに関する情報を、イソクロナスモードのパケットに記録する記録手段（例えば、図2の暗号復号制御回路25）をさらに備えることを特徴とする。

【0019】請求項6に記載のデータ送信装置は、パケットに含ませるデータから所定のデータを時変キーとして抽出する抽出手段（例えば、図2のタイミング回路22）をさらに備えることを特徴とする。

【0020】請求項8に記載のデータ送信装置は、セッションキーに関する情報を、シンクロナスモードのパケットに記録する記録手段（例えば、図2のCPU41）をさらに備えることを特徴とする。

【0021】請求項9に記載のデータ送信装置は、暗号鍵に関する情報を、シリアルバスにおいて、各アイソクロナスサイクルのスタートのタイミングを表すスタートパケットに記録する記録手段（例えば、図2の暗号復号制御回路25）をさらに備えることを特徴とする。

【0022】請求項11に記載のデータ受信装置は、シ

リアルバスを介して送信されてきたデータを受信する受信手段（例えば、図2のPHY部11）と、アイソクロナスモードのパケットにパケット化されているデータをデパケット化するデパケット化手段（例えば、図2の送受信切換回路21）と、アイソクロナスモードのパケットをデパケット化して得たデータであって、暗号化されているデータを復号する復号手段（例えば、図2の暗号化復号化回路24）とを備えることを特徴とする。

【0023】請求項12に記載のデータ受信装置は、パケットのヘッダから、暗号化に関する識別コードを抽出する抽出手段（例えば、図2のヘッダシンク検出生成回路23）をさらに備えることを特徴とする。

【0024】請求項14に記載のデータ受信装置は、時変キーに関する情報を、アイソクロナスモードのパケットから抽出する抽出手段（例えば、図2のヘッダシンク検出生成回路23）をさらに備えることを特徴とする。

【0025】請求項18に記載のデータ受信装置は、セッションキーに関する情報を、シンクロナスモードのパケットから抽出する抽出手段（例えば、図2のCPU41）をさらに備えることを特徴とする。

【0026】請求項20に記載のデータ送受信システムは、データ送信装置は、送信するデータを暗号鍵を用いて暗号化する暗号化手段（例えば、図2の暗号化復号化回路24）と、暗号化手段により暗号化されたデータを、アイソクロナスモードのパケットにパケット化するパケット化手段（例えば、図2の送受信切換回路21）と、パケット化手段によりパケット化されたデータをシリアルバスに送信する送信手段（例えば、図2のPHY部11）とを備え、データ受信装置は、シリアルバスを介して送信されてきたデータを受信する受信手段（例えば、図2のPHY部11）と、アイソクロナスモードのパケットにパケット化されているデータをデパケット化するデパケット化手段（例えば、図2の送受信切換回路21）と、アイソクロナスモードのパケットをデパケット化して得たデータであって、暗号化されているデータを復号する復号手段（例えば、図2の暗号化復号化回路24）とを備えることを特徴とする。

【0027】図1は、本発明を適用した情報処理システムの構成例を表している。このシステムにおいては、デジタルビデオカセットレコーダ1、テレビジョン受像機2、パーソナルコンピュータ3、およびDVDプレーヤ4が、1394バス5により、相互に接続されている。

【0028】図2は、デジタルビデオカセットレコーダ1の内部の構成例を表している。PHY部11は、1394バス5から伝送されてきたデータを受信し、復調して、リンク部12の送受信切換回路21に出力するとともに、送受信切換回路21から供給された送信すべきデータを変調して、1394バス5に出力する。

【0029】リンク部12の送受信切換回路21は、PHY部11から入力された信号をシンクロナスモードの

パケットと、アイソクロナスモードのパケットとに分離し、シンクロナスモードのパケットをデパケット化し、CPU41に出力するとともに、アイソクロナスモードのパケットをデパケット化し、タイミング回路22に出力する。また、CPU41より供給されたシンクロナスモードの信号をパケット化するとともに、タイミング回路22より供給されたデータをアイソクロナスモードのパケットにパケット化して、PHY部11に出力する。

【0030】タイミング回路22は、サイクルタイム3

1、サイクルモニタ32、およびCRC検出生成回路33を内蔵している。サイクルタイム31は、カウンタ34を内蔵しており、このカウンタ34は、所定のクロックをカウントし、125μsのアイソクロナスサイクルのタイミングを表すカウント値を生成する。サイクルモニタ32は、レジスタ35、36を内蔵している。レジスタ35には、1394バス5を介して伝送されてきたサイクルスタートパケットに記録されているデスティネーションオフセット(destination\_offset)の値が保持される。また、レジスタ36は、サイクルスタートパケットのサイクルタイムデータ(cycle\_time\_data)の値が保持される。

【0031】CRC検出生成回路33は、データを受信したとき、誤り検出訂正のためのCRCデータを検出し、これを用いて誤り検出訂正処理を行う。また、データを送信する場合においては、CRC検出生成回路33は、CRCデータを伝送すべきデータに付加する処理を行う。

【0032】ヘッダシンク検出生成回路23は、データ受信時、タイミング回路22より供給されたデータからヘッダとシンクを検出し、これを分離して、実データ部分を暗号化復号化回路24に出力する。また、データを伝送する場合には、暗号化復号化回路24に供給された送信すべきデータに、ヘッダとシンクを附加して、タイミング回路22に出力する。

【0033】暗号化復号化回路24は、データ受信時、ヘッダシンク検出生成回路23より供給されたデータを、暗号復号制御回路25からの制御に対応して復号し、復号結果を記録再生回路42に出力する。また、データ送信時においては、記録再生回路42より入力されたデータを、暗号復号制御回路25からの制御に対応して暗号化し、ヘッダシンク検出生成回路23に出力する。暗号復号制御回路25は、ヘッダシンク検出生成回路23を制御し、ヘッダやデータに所定の識別データを附加させたり、抽出したりする。また暗号復号制御回路25は、暗号化復号化回路24の暗号化または復号化の動作を制御する。

【0034】記録再生回路42は、データ受信時、暗号化復号化回路24より入力されたデータを変調し、ビデオカセット43に記録する。また、再生時、ビデオカセット43に記録されているデータを再生し、復調して、暗号化復号化回路24に出力する。

【0035】図3は、1394バス5に伝送されるデータのタイミングを表している。いま、例えば、デジタルビデオカセットレコーダ1が、ビデオカセット43を再生し、その再生データをテレビジョン受像機2に伝送しているものとする。また、DVDプレーヤ4が、内蔵するDVD(ディスク)から再生したデータを1394バス5を介してパーソナルコンピュータ3に伝送しているものとする。デジタルビデオカセットレコーダ1が、ビデオカセット43を再生して出力するストリームを信号ストリームAとし、DVDプレーヤ4が、DVDを再生して出力するストリームを信号ストリームBとする。

【0036】いま、例えば、1394バス5のサイクルマスタが、デジタルビデオカセットレコーダ1であるとすると、CPU41は、送受信切換回路21を制御し、1394バス5の $125\mu s$ のアイソクロナスサイクルを規定するために、サイクルスタートパケットを発生させる。このサイクルスタートパケットは、図3に示すように、アイソクロナスサイクルの先頭に、S<sub>1</sub>、S<sub>2</sub>、…のよう配置される。

【0037】図6を参照して後述するように、このサイクルスタートパケットには、サイクルタイムデータ(cycle\_time\_data)が配置されている。このサイクルタイムデータには、サイクルタイムマ31のカウンタ34がカウントしているカウント値が記録される。1394バス5に接続されているサイクルマスタ以外の電子機器は、このサイクルタイムデータを読み取り、それを内蔵するサイクルモニタのレジスタに保持させる。

【0038】例えば、サイクルマスタが、デジタルビデオカセットレコーダ1ではなく、パーソナルコンピュータの場合、パーソナルコンピュータ3がサイクルスタートパケットを送信することになる。この場合、デジタルビデオカセットレコーダ1は、1394バス5を介して伝送されてくるサイクルスタートパケットをPHY部11で受信し、送受信切換回路21で、これをデパケット化する。デパケット化されたデータは、タイミング回路22に入力される。タイミング回路22においては、サイクルモニタ32で、このサイクルスタートパケットに含まれるサイクルタイムデータを読み取り、その読み取った値をレジスタ36に保持する。そして、以後、このレジスタ36に保持した値を基準にして、1394バス5上のアイソクロナスサイクルの時間管理を行う。

【0039】このようにして、1394バス5に接続されている各電子機器のアイソクロナスサイクルの時間軸が共通のものとされる。

【0040】いま、デジタルビデオカセットレコーダ1とDVDプレーヤ4が、1394バス5を介してデータを伝送しているので、それぞれは、アイソクロナスサイクルの所定のタイミングにおいて、アイソクロナスパケットを伝送できるようにタイムスロットの割当を受けてい

る。デジタルビデオカセットレコーダ1と、DVDプレーヤ4は、信号ストリームAまたは信号ストリームBを、それぞれ圧縮してパケット化し、パケット化したデータを、それぞれ割当を受けているタイムスロットのタイミングにおいて伝送する。

【0041】例えば、デジタルビデオカセットレコーダ1は、記録再生回路42で、ビデオカセット43を再生し、その再生データを暗号化復号化回路24に供給し、セッションキーSと時変キーiよりなる暗号鍵を用いて暗号化させる。暗号化されたデータは、ヘッダシンク検出生成回路23に供給され、圧縮され、ヘッダが付加される。ヘッダが付加されたデータは、さらにタイミング回路22に入力され、CRCが付加される。このCRCは、ヘッダとデータ部、それぞれに付加される。

【0042】タイミング回路22より出力されたデータは、送受信切換回路21に供給され、アイソクロナスマードのパケットにパケット化される。そして、このパケットは、上述したように、割当を受けたタイムスロットのタイミングにおいて、PHY部11から1394バス5に伝送される。

【0043】このような処理が、図3に示すように、各アイソクロナスサイクル毎に行われ、信号ストリームAの信号A<sub>1</sub>、A<sub>2</sub>、A<sub>3</sub>、…は、各アイソクロナスサイクルの所定のタイムスロットのタイミングで、同一の符号で示すパケットとして送信される。なお、伝送するデータが存在しないアイソクロナスサイクルにおいては、空パケットa<sub>1</sub>、a<sub>2</sub>が伝送される。この空パケットには、実データ部が存在せず、ヘッダ部だけが存在する。

【0044】同様のことが、DVDプレーヤ4においても行われ、信号ストリームBの信号B<sub>1</sub>、B<sub>2</sub>、…が、異なるタイミングで、同一の符号で示すパケットとして伝送される。

【0045】例えば、CPU41がコマンドを送信する場合、そのコマンドが、送受信切換回路21に入力される。送受信切換回路21は、このコマンドをアシンクロナスモードのパケットにパケット化し、例えば、図3においてC<sub>1</sub>、C<sub>2</sub>のように伝送する。

【0046】このアシンクロナスパケットは、必要に応じて伝送されるものであるので、各アイソクロナスサイクルにおいて、常に発生するものではない。

【0047】同様に、CPU41は、後述するように、暗号鍵のうち、セッションキーSを、アシンクロナスパケットで伝送する。

【0048】このように、1394バス5を介して伝送された信号ストリームAは、テレビジョン受像機2で受信され、信号ストリームBは、パーソナルコンピュータ3で受信されるのであるが、説明の便宜上、いま信号ストリームAが、図2に示すデジタルビデオカセットレコーダ1で受信されるものとすると、そのときの動作は次

のようになる。

【0049】すなわち、PHY部11は、1394バス5を介して伝送されてきたパケットを受信し、送受信切換回路21に供給する。送受信切換回路21は、入力されたパケットをアイソクロナスパケットとアシンクロナスパケットに分離し、アイソクロナスパケットをデパケット化して、タイミング回路22に出力し、アシンクロナスパケットをデパケット化し、そのデータをCPU41に出力する。その結果、例えば、タイミング回路22に信号ストリームAが供給され、CPU41にコマンドやセッションキーSが供給される。

【0050】タイミング回路22のCRC検出生成回路33は、入力されたデータをヘッダシンク検出生成回路23に供給する。そして、CRC検出生成回路33は、ヘッダシンク検出生成回路23に供給されたデータからCRCを検出し、これを用いて、誤り検出訂正処理を実行する。そして、誤りが訂正されたデータをヘッダシンク検出生成回路23に戻す。

【0051】ヘッダシンク検出生成回路23は、入力されたデータからヘッダを分離し、ヘッダ情報を暗号復号制御回路25に供給し、実データ部を暗号化復号化回路24に供給する。暗号復号制御回路25は、ヘッダシンク検出生成回路23が検出したヘッダに含まれる暗号化の識別データを検出し、この検出結果に対して、暗号化復号化回路24を制御する。すなわち、この識別データが、データが暗号化されていることを示している場合には、暗号化復号化回路24を制御し、暗号鍵を用いて復号処理を実行させる。識別データが、データが暗号化されていないことを示している場合には、暗号化処理を省略させる。

【0052】暗号化復号化回路24より出力されたデータは、記録再生回路42により、所定の方式で変調され、ビデオカセット43に供給され、記録される。

【0053】なお、この発明の実施の形態においては、暗号化復号化回路24における、暗号化と復号化に用いられる暗号鍵が、セッションキーSと、時変キーiにより構成されている。セッションキーSは、セッション毎に（例えば、1つの映画情報毎に、あるいは、1回の再生毎に）、適宜更新される。換言すれば、同一のセッション内においては、不変の値とされる。これに対して、時変キーiは、1つのセッション内において、頻繁に更新される。このように、セッションキーSと時変キーiを暗号鍵として、より安全性を高めることができる。

【0054】すなわち、例えば、セッションキーSが盗まれたとしても、時変キーiが不明であれば、結局暗号化されているデータを復号することができない。さらに、時変キーiも盗まれたとしても、時変キーiは、時々刻々と更新されるので、極めて短い時間の間だけデータを復号することができるが、それ以降は、データを復

号することができなくなる。

【0055】セッションキーSは、図3にK<sub>1</sub>、K<sub>2</sub>として示すように、所定のタイミングで、アシンクロナスパケットとして伝送される。勿論、後述するように、時変キーiと同様に、アイソクロナスパケットとして伝送することも可能である。

10

【0056】図4は、アイソクロナスパケットのフォーマットを表している。同図に示すように、その先頭の2クワドレットは、アイソクロナスヘッダとされる。このヘッダの先頭には、データ長(data\_length)が記録され、その次には、データフィールド(data field)中にCIPヘッダが付加されているか否かを表すtagが記録されている。tagの次には、channel1が配置される。このchannelは、例えば、図3におけるストリームAやストリームBの識別を行うものである。

20

【0057】tcodは、パケットフォーマットを規定するものであり、アイソクロナススタートパケットの場合、1010(=A)とされる。次のsyは、シンクロナイジエーションコードとされ、アプリケーション毎に規定される。本発明の実施の形態においては、このsyの下位2ビットに、32ビット乃至40ビットで構成される時変キーiの2ビット分が配置される。例えば、時変キーiが32ビットにより構成される場合、16パケットを集めて時変キーiが完成することになる。syの下から3ビット目には、このパケットが時変キーiの先頭のパケットであるか否かを示すフラグを附加することができる。例えば、時変キーiの先頭である場合、この3番目のビットが1とされ、先頭でない場合、0とされる。

30

【0058】さらに、このようにsyに時変キーiを記録する場合、tcodに、値1100(=C)を設定し、時変キーiの識別コードとすることができます。

40

【0059】暗号復号制御回路25は、ヘッダシンク検出生成回路23の出力するヘッダ情報から、この時変キーiを2ビットずつ集め、16パケット分集めたとき、完成した時変キーiを暗号化復号化回路24に転送することになる。

【0060】図4に示すように、アイソクロナスヘッダの2番目のクワドレットは、ヘッダCRCとされている。そして、アイソクロナスヘッダの次のデータフィールドには、2クワドレット分のCIPヘッダが配置され、その次に、コンテンツが配置される。このコンテンツが、上述したように、暗号化されたデータとなる。

【0061】なお、MPEGの場合、このコンテンツの領域に、ソースヘッダが配置されるが、このタイムスタンプなどが記録されているソースヘッダは、暗号化しないようにする。

【0062】データフィールドの次には、データCRCが配置されている。

50

【0063】図5は、CIPヘッダの詳細な構成を表している。同図に示すように、2クワドレットのCIPヘッダ

のうち、最初のCIPヘッダ1においては、その先頭に、ヘッダの先頭であることを表すビット(=0)が配置され、CIPヘッダ2においては、ここにビット1が配置される。すなわち、最初のビットは、EOH\_n(End of CIP header)とされ、これは、CIPヘッダの最後のクロードレットであるか否かを表している。この値は、他のクロードレットが続く場合、0とされ、CIPヘッダの最後のクロードレットである場合、1とされる。

【0064】第2番目のビットは、Form\_nとされ、これは、EOHと組み合わせることで、CIPヘッダフィールドのクロードレットを表すようになされているが、この発明の実施の形態においては、データが暗号化されている場合、ここに1が設定され、暗号化されていない場合、0が記録される。

【0065】CIPヘッダ1の第3番目乃至第8番目のビットは、SID(Source node ID)とされる。SIDの次には、DBS(Data block size in quadlets)が配置される。このDBSは、データのブロックサイズを表している。その次には、FN(Fraction number)が配置されている。これは、1つのソースパケットが分割されているブロックの数を表している。次の、QPC(Quadlet padding count)は、付加されたダミークロードレットの数を表している。次のSPH(Source packet header)は、ソースパケットがソースパケットヘッダを有しているか否かを表している。

【0066】Rsvは、将来のために保留されている。DBCは、データブロックの損失を検知するための連続するデータブロックのカウンタの値を表している。

【0067】FMTは、Format IDを表している。FDFは、Format dependent fieldを表している。

【0068】図6は、サイクルスタートパケットのフォーマットを表している。その先頭には、destination\_IDが配置され、これは、データ転送先のIDを表している。次のtl(transaction label)は、通常すべて0とされる。そこで、例えば、ここに時変キーiの値を記録するようになることができる。

【0069】rt(retry code)は、通常0とされる。次の、tcode(transactin code)には、パケットタイプのtransaction codeが配置される。

【0070】priは、priorityであり、1394バス5で接続される機器間で使用されるとき、すべて1とされる。このpriにも、時変キーiを割り当てることが可能である。

【0071】source\_IDには、データの伝送元のIDが記録される。destination\_offsetには、サイクルスタートパケットからのタイミングのずれに対応するクロックの値がセットされる。cycle\_time\_dataには、上述したように、サイクルマスターの基準となるレジスタの値が設定される。この値を基準として、1394バス5に接続されている各電子機器のアイソクロナスサイクルの時間軸

の基準が設定される。一番最後には、ヘッダのCRCが配置されている。

【0072】以上の実施の形態においては、時変キーiを、パケットのデータ部またはヘッダ部に書き込んで伝送するようにしたが、例えば、サイクルスタートパケットのdestination\_offset, cycle\_time\_dataまたはheader\_CRCのいずれかの値を、そのまま時変キーiとして用いるようにすることもできる。

【0073】また、各電子機器は、これらの値を読み取って、そのサイクルモニタ32のレジスタ35, 36に、これらの値を保持しているので、これらの値から時変キーiを抽出するようにすることも可能である。

【0074】さらにまた、図5に示したCIPヘッダのDBC、図4に示したdata\_CRCの値を、そのまま時変キーiとして用いるようにすることもできる。

【0075】

【発明の効果】以上の如く、請求項1に記載のデータ送信装置および請求項10に記載のデータ送信方法によれば、暗号化されたデータを、アイソクロナスマードのパケットにパケット化して、シリアルバスに送信するようにしたので、より安全にデータを送信することが可能となる。

【0076】請求項11に記載のデータ受信装置および請求項19に記載のデータ受信方法によれば、アイソクロナスマードのパケットでパケット化して得たデータであって、暗号化されているデータを復号するようにしたので、安全に伝送されてきたデータを、確実に復号することが可能となる。

【0077】請求項20に記載のデータ送受信システムおよび請求項21に記載のデータ送受信方法によれば、データ送信装置で暗号化されたデータを、アイソクロナスマードのパケットにパケット化して送信し、データ受信装置において、これを受信するようにしたので、安全なデータ送受信システムを実現することができる。

【図面の簡単な説明】

【図1】本発明を適用したデータ送受信システムの構成例を示すブロック図である。

【図2】図1のデジタルビデオカセットレコーダ1の内部の構成例を示すブロック図である。

【図3】1394バスの伝送のタイミングを説明する図である。

【図4】アイソクロナスパケットのフォーマットを示す図である。

【図5】CIPヘッダのフォーマットを示す図である。

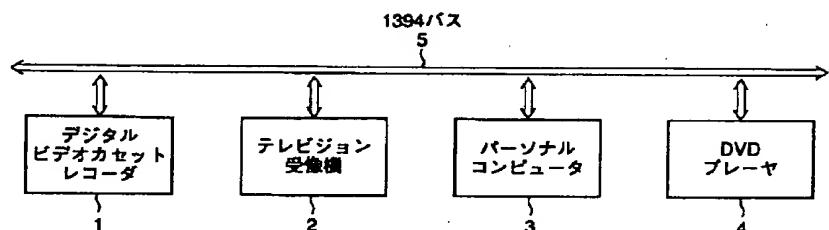
【図6】サイクルスタートパケットのフォーマットを示す図である。

【符号の説明】

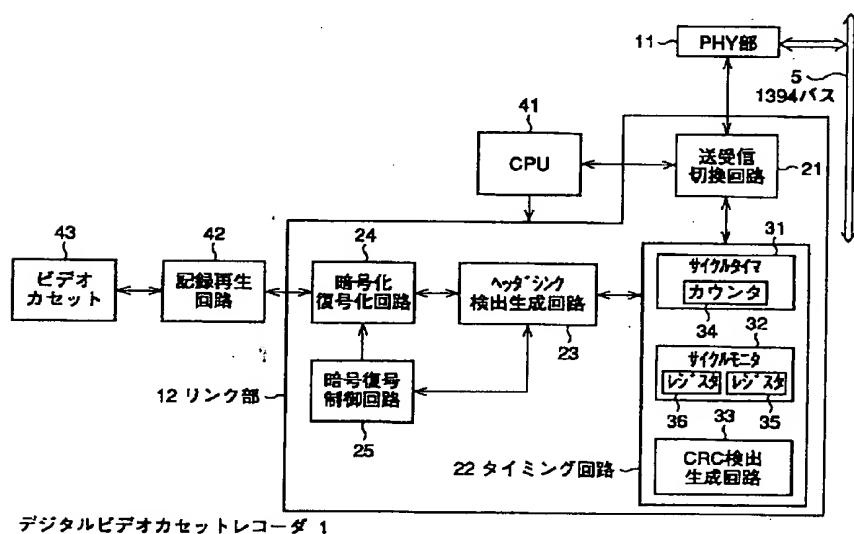
1 デジタルビデオカセットレコーダ, 2 テレビジョン受像機, 3 パーソナルコンピュータ, 4 DV Dプレーヤ, 5 1394バス, 11 PHY部, 1

2 リンク部, 21 送受信切換回路, 22 タイミング回路, 23 ヘッダシンク検出生成回路, 24 暗号化復号化回路, 25 暗号復号制御回路, 31 サイクルタイマ, 32 サイクルモニタ, 33 CRC検出生成回路, 34 カウンタ, 35, 36 レジスタ, 41 CPU

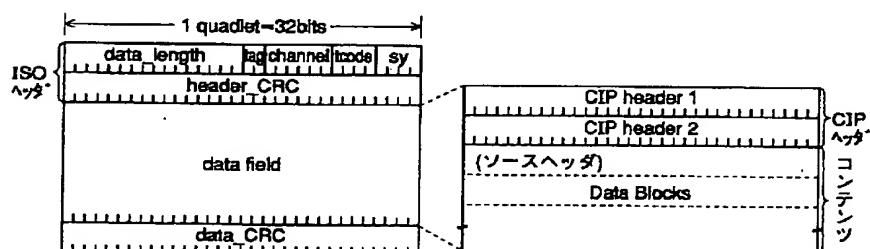
【図1】



【図2】

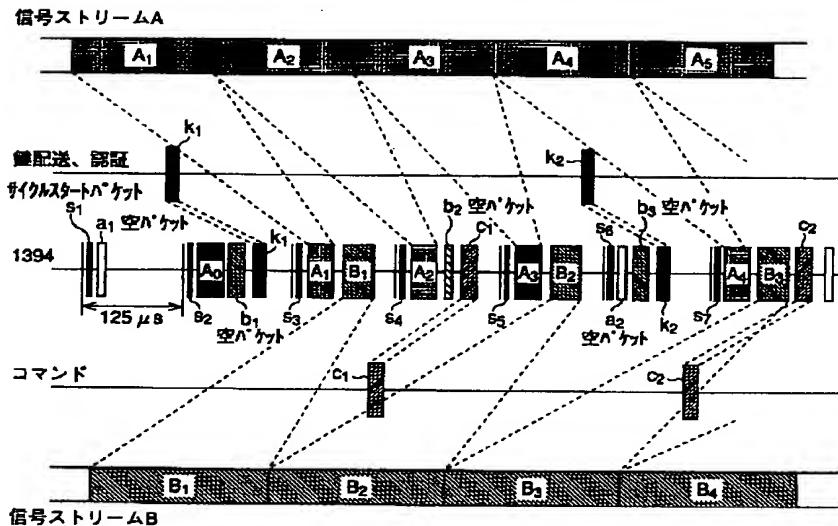


【図4】

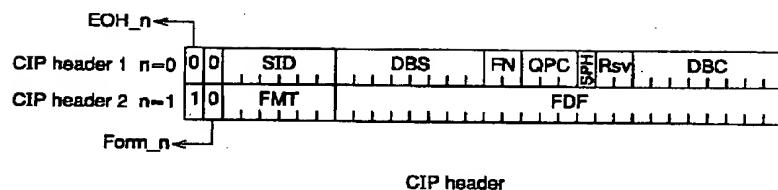


Isochronous packet

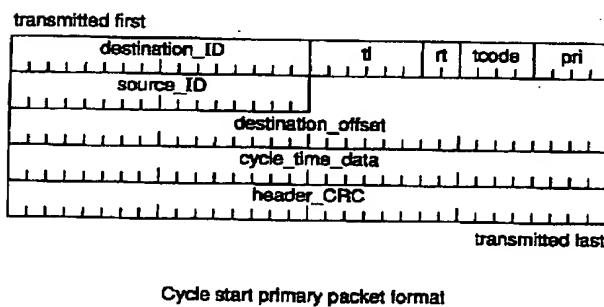
【図3】



【図5】



【図6】



Cycle start primary packet format

フロントページの続き

(51) Int. Cl. <sup>6</sup>  
 H 04 L 9/16  
 12/56

識別記号

F I  
 H 04 L 9/00  
 11/20 6 4 3  
 102 F

(72) 発明者 浅野 智之  
東京都品川区北品川6丁目7番35号 ソニ  
一株式会社内

(72) 発明者 石黒 隆二  
東京都品川区北品川6丁目7番35号 ソニ  
一株式会社内

(72) 発明者 嶋 久登  
アメリカ合衆国 カリフォルニア州 サラ  
トガ パセオ・フローレス12610

【公報種別】特許法第17条の2の規定による補正の掲載

【部門区分】第7部門第3区分

【発行日】平成16年11月4日(2004.11.4)

【公開番号】特開平10-303945

【公開日】平成10年11月13日(1998.11.13)

【出願番号】特願平9-106105

【国際特許分類第7版】

H 04 L 12/40

G 11 B 20/10

H 04 L 9/08

H 04 L 9/14

H 04 L 9/16

H 04 L 12/56

【F 1】

H 04 L 11/00 320

G 11 B 20/10 H

G 11 B 20/10 D

H 04 L 9/00 601C

H 04 L 9/00 641

H 04 L 9/00 643

H 04 L 11/20 102F

【手続補正書】

【提出日】平成15年11月6日(2003.11.6)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

シリアルバスで接続された情報処理装置に、実時間データ伝送と非同期データ伝送によりデータを送信するデータ送信装置において、送信するコンテンツデータを、各セッションにおいて不变なセッションキーと、前記セッション内において更新される時変キーとからなる暗号鍵を用いて暗号化する暗号化手段と、前記暗号化手段により暗号化された前記コンテンツデータにヘッダを付加し、前記実時間データ伝送のパケットにパケット化するパケット化手段と、前記パケット化手段により前記実時間データ伝送のパケットにパケット化されたデータを前記シリアルバスに送信する送信手段とを備えることを特徴とするデータ送信装置。

【請求項2】

前記パケット化手段により付加されたヘッダに、前記暗号化に関する識別コードを書き込む書き込み手段を

さらに備えることを特徴とする請求項1に記載のデータ送信装置。

【請求項3】

前記時変キーに関する情報を、前記パケット化手段により付加された前記ヘッダに書き込む書き込み手段を

さらに備えることを特徴とする請求項1に記載のデータ送信装置。

## 【請求項 4】

前記パケット化手段は、さらに、前記セッションキーに関する情報を、前記非同期データ伝送のパケットにパケット化し、

前記送信手段は、前記パケット化手段により前記非同期データ伝送のパケットにパケット化されたデータもさらに前記シリアルバスに送信する

ことを特徴とする請求項1に記載のデータ送信装置。

## 【請求項 5】

前記送信手段は、前記実時間データ伝送を、前記シリアルバスのアイソクロナスマードのパケット伝送により行い、前記非同期データ伝送を、前記シリアルバスのアシンクロナスマードのパケット伝送により行う

ことを特徴とする請求項1に記載のデータ送信装置。

## 【請求項 6】

前記送信手段は、前記シリアルバスとしてのIEEE1394の前記アイソクロナスマードと前記アシンクロナスマードに基づいて前記パケットの伝送を行う

ことを特徴とする請求項5に記載のデータ送信装置。

## 【請求項 7】

シリアルバスで接続された情報処理装置に、実時間データ伝送と非同期データ伝送によりデータを送信するデータ送信方法において、

送信するコンテンツデータを、各セッションにおいて不变なセッションキーと、前記セッション内において更新される時変キーとからなる暗号鍵を用いて暗号化する暗号化ステップと、

前記暗号化ステップの処理により暗号化された前記コンテンツデータにヘッダを付加し、前記実時間データ伝送のパケットにパケット化するパケット化ステップと、

前記パケット化ステップの処理により前記実時間データ伝送のパケットにパケット化されたデータを前記シリアルバスに送信する送信ステップと

を備えることを特徴とするデータ送信方法。

## 【請求項 8】

シリアルバスで接続されたデータ送信装置から、実時間データ伝送と非同期データ伝送により送信してきたデータを受信するデータ受信装置において、

前記シリアルバスを介して送信してきたデータを受信する受信手段と、

前記実時間データ伝送のパケットにパケット化されているデータをデパケット化するデパケット化手段と、

前記実時間データ伝送のパケットをデパケット化して得たデータであって、暗号化されているデータを、各セッションにおいて不变なセッションキーと、前記セッション内において更新される時変キーとからなる暗号鍵を用いて復号する復号手段とを備えることを特徴とするデータ受信装置。

## 【請求項 9】

前記実時間データ伝送のパケットのヘッダから、前記暗号化に関する識別コードを抽出する抽出手段を

さらに備えることを特徴とする請求項8に記載のデータ受信装置。

## 【請求項 10】

前記時変キーに関する情報を、前記実時間データ伝送のパケットのヘッダから抽出する抽出手段を

さらに備えることを特徴とする請求項8に記載のデータ受信装置。

## 【請求項 11】

前記デパケット化手段は、前記非同期データ伝送のパケットにパケット化されているデータもさらにデパケット化し、

前記セッションキーに関する情報を、前記非同期データ伝送のパケットから抽出する抽出手段を

さらに備えることを特徴とする請求項8に記載のデータ受信装置。

**【請求項 1 2】**

前記受信手段は、前記実時間データ伝送が、前記シリアルバスのアイソクロナスマードのパケット伝送により行われ、前記非同期データ伝送が、前記シリアルバスのアシンクロナスマードのパケット伝送により行われたデータを受信することを特徴とする請求項8に記載のデータ受信装置。

**【請求項 1 3】**

前記受信手段は、前記シリアルバスとしてのIEEE1394の前記アイソクロナスマードと前記アシンクロナスマードに基づいて送信されてきた前記パケットを受信することを特徴とする請求項12に記載のデータ受信装置。

**【請求項 1 4】**

シリアルバスで接続されたデータ送信装置から、実時間データ伝送と非同期データ伝送により送信されてきたデータを受信するデータ受信方法において、前記シリアルバスを介して送信されてきたデータを受信する受信ステップと、前記実時間データ伝送のパケットにパケット化されているデータをデパケット化するデパケット化ステップと、前記実時間データ伝送のパケットをデパケット化して得たデータであって、暗号化されているデータを、各セッションにおいて不变なセッションキーと、前記セッション内において更新される時変キーとからなる暗号鍵を用いて復号する復号ステップとを備えることを特徴とするデータ受信方法。

**【請求項 1 5】**

シリアルバスで接続されたデータ送信装置と、前記データ送信装置が、実時間データ伝送と非同期データ伝送により送信したデータを受信するデータ受信装置とを備えるデータ送受信システムにおいて、

前記データ送信装置は、

送信するコンテンツデータを、各セッションにおいて不变なセッションキーと、前記セッション内において更新される時変キーとからなる暗号鍵を用いて暗号化する暗号化手段と、

前記暗号化手段により暗号化された前記コンテンツデータにヘッダを付加し、前記実時間データ伝送のパケットにパケット化するパケット化手段と、

前記パケット化手段により前記実時間データ伝送のパケットにパケット化されたデータを前記シリアルバスに送信する送信手段とを備え、

前記データ受信装置は、

前記シリアルバスを介して送信されてきたデータを受信する受信手段と、

前記実時間データ伝送のパケットにパケット化されているデータをデパケット化するデパケット化手段と、

前記実時間データ伝送のパケットをデパケット化して得たデータであって、暗号化されているデータを、前記暗号鍵を用いて復号する復号手段とを備える

ことを特徴とするデータ送受信システム。

**【請求項 1 6】**

前記送信手段は、前記実時間データ伝送を、前記シリアルバスのアイソクロナスマードのパケット伝送により行い、前記非同期データ伝送を、前記シリアルバスのアシンクロナスマードのパケット伝送により行い、

前記受信手段は、前記アイソクロナスマードと前記アシンクロナスマードのパケット伝送により送信されてきたデータを受信する

ことを特徴とする請求項15に記載のデータ送受信システム。

**【請求項 1 7】**

前記送信手段は、前記シリアルバスとしてのIEEE1394の前記アイソクロナスマードと前記アシンクロナスマードに基づいて前記パケットの伝送を行い、

前記受信手段は、前記シリアルバスとしての IEEE 1394 の前記アイソクロナスマードと前記シンクロナスマードに基づいて送信されてきた前記パケットを受信することを特徴とする請求項 16 に記載のデータ送受信システム。

【請求項 18】

シリアルバスで接続されたデータ送信装置と、前記データ送信装置が、実時間データ伝送と非同期データ伝送により送信したデータを受信するデータ受信装置とを備えるデータ送受信システムのデータ送受信方法において、

前記データ送信装置は、

送信するコンテンツデータを、各セッションにおいて不变なセッションキーと、前記セッション内において更新される時変キーとからなる暗号鍵を用いて暗号化する暗号化ステップと、

前記暗号化ステップの処理により暗号化された前記コンテンツデータにヘッダを付加し、前記実時間データ伝送のパケットにパケット化するパケット化ステップと、

前記パケット化ステップの処理により前記実時間データ伝送のパケットにパケット化されたデータを前記シリアルバスに送信する送信ステップとを備え、

前記データ受信装置は、

前記シリアルバスを介して送信されてきたデータを受信する受信ステップと、

前記実時間データ伝送のパケットにパケット化されているデータをデパケット化するデパケット化ステップと、

前記実時間データ伝送のパケットをデパケット化して得たデータであって、暗号化されているデータを、前記暗号鍵を用いて復号する復号ステップとを備える

ことを特徴とするデータ送受信方法。

【手続補正 2】

【補正対象書類名】明細書

【補正対象項目名】0006

【補正方法】変更

【補正の内容】

【0006】

【課題を解決するための手段】

請求項 1 に記載のデータ送信装置は、送信するコンテンツデータを、各セッションにおいて不变なセッションキーと、セッション内において更新される時変キーとからなる暗号鍵を用いて暗号化する暗号化手段と、暗号化手段により暗号化されたコンテンツデータにヘッダを付加し、実時間データ伝送のパケットにパケット化するパケット化手段と、パケット化手段により実時間データ伝送のパケットにパケット化されたデータをシリアルバスに送信する送信手段とを備えることを特徴とする。

【手続補正 3】

【補正対象書類名】明細書

【補正対象項目名】0007

【補正方法】変更

【補正の内容】

【0007】

請求項 7 に記載のデータ送信方法は、送信するコンテンツデータを、各セッションにおいて不变なセッションキーと、セッション内において更新される時変キーとからなる暗号鍵を用いて暗号化する暗号化ステップと、暗号化ステップの処理により暗号化されたコンテンツデータにヘッダを付加し、実時間データ伝送のパケットにパケット化するパケット化ステップと、パケット化ステップの処理により実時間データ伝送のパケットにパケット化されたデータをシリアルバスに送信する送信ステップとを備えることを特徴とする。

【手続補正 4】

【補正対象書類名】明細書

【補正対象項目名】0008

【補正方法】変更

【補正の内容】

【0008】

請求項8に記載のデータ受信装置は、シリアルバスを介して送信されてきたデータを受信する受信手段と、実時間データ伝送のパケットにパケット化されているデータをデパケット化するデパケット化手段と、実時間データ伝送のパケットをデパケット化して得たデータであって、暗号化されているデータを、各セッションにおいて不変なセッションキーと、セッション内において更新される時変キーとからなる暗号鍵を用いて復号する復号手段とを備えることを特徴とする。

【手続補正5】

【補正対象書類名】明細書

【補正対象項目名】0009

【補正方法】変更

【補正の内容】

【0009】

請求項14に記載のデータ受信方法は、シリアルバスを介して送信されてきたデータを受信する受信ステップと、実時間データ伝送のパケットにパケット化されているデータをデパケット化するデパケット化ステップと、実時間データ伝送のパケットをデパケット化して得たデータであって、暗号化されているデータを、各セッションにおいて不変なセッションキーと、セッション内において更新される時変キーとからなる暗号鍵を用いて復号する復号ステップとを備えることを特徴とする。

【手続補正6】

【補正対象書類名】明細書

【補正対象項目名】0010

【補正方法】変更

【補正の内容】

【0010】

請求項15に記載のデータ送受信システムは、データ送信装置は、送信するコンテンツデータを、各セッションにおいて不変なセッションキーと、セッション内において更新される時変キーとからなる暗号鍵を用いて暗号化する暗号化手段と、暗号化手段により暗号化されたコンテンツデータにヘッダを付加し、実時間データ伝送のパケットにパケット化するパケット化手段と、パケット化手段により実時間データ伝送のパケットにパケット化されたデータをシリアルバスに送信する送信手段とを備え、データ受信装置は、シリアルバスを介して送信されてきたデータを受信する受信手段と、実時間データ伝送のパケットにパケット化されているデータをデパケット化するデパケット化手段と、実時間データ伝送のパケットをデパケット化して得たデータであって、暗号化されているデータを、暗号鍵を用いて復号する復号手段とを備えることを特徴とする。

【手続補正7】

【補正対象書類名】明細書

【補正対象項目名】0011

【補正方法】変更

【補正の内容】

【0011】

請求項18に記載のデータ送受信方法は、データ送信装置は、送信するコンテンツデータを、各セッションにおいて不変なセッションキーと、セッション内において更新される時変キーとからなる暗号鍵を用いて暗号化する暗号化ステップと、暗号化ステップの処理により暗号化されたコンテンツデータにヘッダを付加し、実時間データ伝送のパケットにパケット化するパケット化ステップと、パケット化ステップの処理により実時間データ伝送

のパケットにパケット化されたデータをシリアルバスに送信する送信ステップとを備え、データ受信装置は、シリアルバスを介して送信されてきたデータを受信する受信ステップと、実時間データ伝送のパケットにパケット化されているデータをデパケット化するデパケット化ステップと、実時間データ伝送のパケットをデパケット化して得たデータであって、暗号化されているデータを、暗号鍵を用いて復号する復号ステップとを備えることを特徴とする。

【手続補正8】

【補正対象書類名】明細書

【補正対象項目名】0012

【補正方法】変更

【補正の内容】

【0012】

請求項1に記載のデータ送信装置および請求項7に記載のデータ送信方法においては、コンテンツデータが、各セッションにおいて不変なセッションキーと、セッション内において更新される時変キーとからなる暗号鍵を用いて暗号化され、暗号化されたコンテンツデータにヘッダが付加され、実時間データ伝送のパケットにパケット化され、シリアルバスに送信される。

【手続補正9】

【補正対象書類名】明細書

【補正対象項目名】0013

【補正方法】変更

【補正の内容】

【0013】

請求項8に記載のデータ受信装置および請求項14に記載のデータ受信方法においては、シリアルバスを介して送信されてきたデータが受信され、実時間データ伝送のパケットにパケット化されているデータがデパケット化され、実時間データ伝送のパケットをデパケット化して得たデータであって、暗号化されているデータが、各セッションにおいて不変なセッションキーと、前記セッション内において更新される時変キーとからなる暗号鍵を用いて復号される。

【手続補正10】

【補正対象書類名】明細書

【補正対象項目名】0014

【補正方法】変更

【補正の内容】

【0014】

請求項15に記載のデータ送受信システムおよび請求項18に記載のデータ送受信方法においては、データ送信装置が、コンテンツデータを、各セッションにおいて不変なセッションキーと、セッション内において更新される時変キーとからなる暗号鍵を用いて暗号化し、暗号化されたコンテンツデータにヘッダを付加し、実時間データ伝送のパケットにパケット化し、シリアルバスでデータ受信装置に送信する。データ受信装置は、シリアルバスを介して送信されてきたデータを受信し、実時間データ伝送のパケットにパケット化されているデータをデパケット化し、実時間データ伝送のパケットをデパケット化して得たデータであって、暗号化されているデータを、暗号鍵を用いて復号する。

【手続補正11】

【補正対象書類名】明細書

【補正対象項目名】0016

【補正方法】変更

【補正の内容】

【0016】

請求項1に記載のデータ送信装置は、送信するコンテンツデータ（例えば、映像信号や音

声信号)を、各セッションにおいて不变なセッションキー(例えば、セッションキーS)と、セッション内において更新される時変キー(例えば、時変キーi)とからなる暗号鍵を用いて暗号化する暗号化手段(例えば、図2の暗号化復号化回路24)と、暗号化手段により暗号化されたコンテンツデータにヘッダを付加し、実時間データ伝送のパケットにパケット化するパケット化手段(例えば、図2の送受信切換回路21)と、パケット化手段により実時間データ伝送のパケットにパケット化されたデータをシリアルバスに送信する送信手段(例えば、図2のPHY部11)とを備えることを特徴とする。

【手続補正12】

【補正対象書類名】明細書

【補正対象項目名】0017

【補正方法】変更

【補正の内容】

【0017】

請求項2に記載のデータ送信装置は、パケット化手段により付加されたヘッダに、暗号化に関する識別コード(例えば、tcode)を書き込む書き込み手段(例えば、図2の暗号復号制御回路25)をさらに備えることを特徴とする。

【手続補正13】

【補正対象書類名】明細書

【補正対象項目名】0018

【補正方法】変更

【補正の内容】

【0018】

請求項3に記載のデータ送信装置は、時変キーに関する情報を、パケット化手段により付加されたヘッダに書き込む書き込み手段(例えば、図2の暗号復号制御回路25)をさらに備えることを特徴とする。

【手続補正14】

【補正対象書類名】明細書

【補正対象項目名】0019

【補正方法】削除

【補正の内容】

【手続補正15】

【補正対象書類名】明細書

【補正対象項目名】0020

【補正方法】削除

【補正の内容】

【手続補正16】

【補正対象書類名】明細書

【補正対象項目名】0021

【補正方法】削除

【補正の内容】

【手続補正17】

【補正対象書類名】明細書

【補正対象項目名】0022

【補正方法】変更

【補正の内容】

【0022】

請求項8に記載のデータ受信装置は、シリアルバスを介して送信されてきたデータを受信

する受信手段（例えば、図2のPHY部11）と、実時間データ伝送のパケットにパケット化されているデータをデパケット化するデパケット化手段（例えば、図2の送受信切換回路21）と、実時間データ伝送のパケットをデパケット化して得たデータであって、暗号化されているデータを、各セッションにおいて不変なセッションキー（例えば、セッションキーS）と、セッション内において更新される時変キー（例えば、時変キーi）とからなる暗号鍵を用いて復号する復号手段（例えば、図2の暗号化復号化回路24）とを備えることを特徴とする。

【手続補正18】

【補正対象書類名】明細書

【補正対象項目名】0023

【補正方法】変更

【補正の内容】

【0023】

請求項9に記載のデータ受信装置は、パケットのヘッダから、暗号化に関する識別コード（例えば、tcode）を抽出する抽出手段（例えば、図2のヘッダシンク検出生成回路23）をさらに備えることを特徴とする。

【手続補正19】

【補正対象書類名】明細書

【補正対象項目名】0024

【補正方法】変更

【補正の内容】

【0024】

請求項10に記載のデータ受信装置は、時変キーに関する情報を、実時間データ伝送のパケットのヘッダから抽出する抽出手段（例えば、図2のヘッダシンク検出生成回路23）をさらに備えることを特徴とする。

【手続補正20】

【補正対象書類名】明細書

【補正対象項目名】0025

【補正方法】変更

【補正の内容】

【0025】

請求項11に記載のデータ受信装置は、デパケット化手段は、非同期データ伝送のパケットにパケット化されているデータもさらにデパケット化し、セッションキーに関する情報を、非同期データ伝送のパケットから抽出する抽出手段（例えば、図2のCPU41）をさらに備えることを特徴とする。

【手続補正21】

【補正対象書類名】明細書

【補正対象項目名】0026

【補正方法】変更

【補正の内容】

【0026】

請求項15に記載のデータ送受信システムは、データ送信装置は、送信するコンテンツデータ（例えば、映像信号や音声信号）を、各セッションにおいて不変なセッションキー（例えば、セッションキーS）と、セッション内において更新される時変キー（例えば、時変キーi）とからなる暗号鍵を用いて暗号化する暗号化手段（例えば、図2の暗号化復号化回路24）と、暗号化手段により暗号化されたコンテンツデータにヘッダを付加し、実時間データ伝送のパケットにパケット化するパケット化手段（例えば、図2の送受信切換回路21）と、パケット化手段により実時間データ伝送のパケットにパケット化されたデータをシリアルバスに送信する送信手段（例えば、図2のPHY部11）とを備え、データ受信装置は、シリアルバスを介して送信されてきたデータを受信する受信手段（例えば、

図2のPHY部11)と、実時間データ伝送のパケットにパケット化されているデータをデパケット化するデパケット化手段(例えば、図2の送受信切換回路21)と、実時間データ伝送のパケットをデパケット化して得たデータであって、暗号化されているデータを、暗号鍵を用いて復号する復号手段(例えば、図2の暗号化復号化回路24)とを備えることを特徴とする。

【手続補正22】

【補正対象書類名】明細書

【補正対象項目名】0075

【補正方法】変更

【補正の内容】

【0075】

【発明の効果】

以上の如く、請求項1に記載のデータ送信装置および請求項7に記載のデータ送信方法によれば、暗号化されたデータを、実時間データ伝送のパケットにパケット化して、シリアルバスに送信するようにしたので、より安全にデータを送信することが可能となる。

【手続補正23】

【補正対象書類名】明細書

【補正対象項目名】0076

【補正方法】変更

【補正の内容】

【0076】

請求項8に記載のデータ受信装置および請求項14に記載のデータ受信方法によれば、実時間データ伝送のパケットでパケット化して得たデータであって、暗号化されているデータを復号するようにしたので、安全に伝送されてきたデータを、確実に復号することが可能となる。

【手続補正24】

【補正対象書類名】明細書

【補正対象項目名】0077

【補正方法】変更

【補正の内容】

【0077】

請求項15に記載のデータ送受信システムおよび請求項18に記載のデータ送受信方法によれば、データ送信装置で暗号化されたデータを、実時間データ伝送のパケットにパケット化して送信し、データ受信装置において、これを受信するようにしたので、安全なデータ送受信システムを実現することができる。